

FILED
2005 MAY 16 PM 2:10
U.S. DISTRICT COURT
CENTRAL DISTRICT OF CALIF.

UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA,) Case No. CR 04-704(B)
Plaintiff,) ~~AMENDED~~
v.) FIRST
PAUL GARRETT ASHLEY,) SUPERSEEDING
Defendant.) INFORMATION
[18 U.S.C. § 371: Conspiracy;
18 U.S.C. §§ 1030(a)(5)(A)(i) and
2: Aiding and Abetting the
Transmission of a Code,
Information, Program or Command
to a Protected Computer]

The United States Attorney charges:

INTRODUCTORY ALLEGATIONS

At all times relevant to this information:

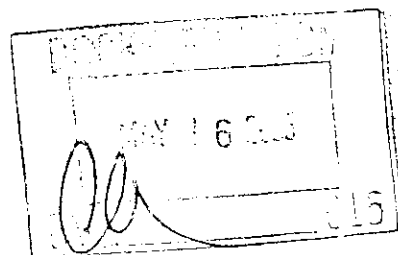
ASHLEY

1. Defendant PAUL GARRETT ASHLEY was the founder, owner, and computer systems administrator of Creative Internet Techniques ("CIT"), an Internet Service Provider based in Powell, Ohio. CIT ran a network known as "Foonet" that provided web hosting and other computer services to customers.

//

//

JMA:jma



51

1 ECHOUAFNI

2 2. In December 2003, ASHLEY sold CIT to one of his CIT
3 clients, Jay R. Echouafni, also known as ("a.k.a.") Saad Echouafni,
4 the owner and Chief Executive Officer of Orbit Communication
5 Corporation ("Orbit"), a Massachusetts corporation based in
6 Sudbury, Massachusetts. Orbit provided home satellite systems to
7 customers through its website, www.orbitsat.com, and its sales
8 department. Echouafni retained ASHLEY as the network administrator
9 of CIT after December 2003.

10 WEAKNEES

11 3. Weaknees was an online business based in Los Angeles,
12 California, that sold and upgraded personal digital video recorders
13 ("DVRs") including "TIVO" and other DVRs. Weaknees sold its
14 products through its website on the Internet, www.weaknees.com.
15 Weaknees had a strategic alliance with Rapid Satellite.

16 RAPID SATELLITE

17 4. Rapid Satellite was an online business owned by WebClick
18 Concepts Inc. in Miami, Florida. Rapid Satellite sold home
19 satellite television systems to customers through its website,
20 www.rapidsatellite.com, and sales department. Rapid Satellite was
21 a competitor of Orbit.

22 EXPERT SATELLITE

23 5. Expert Satellite was an online business based in
24 Worcester, Massachusetts, that sold home satellite television
25 systems to customers through its website and sales department.
26 Expert's website, www.expertsatellite.com, was available to
27 customers over the Internet. Expert Satellite was a competitor of
28 Orbit.

1 UNINDICTED CO-CONSPIRATOR IN METAIRIE, LOUISIANA

2 6. An unindicted co-conspirator residing in Metairie,
3 Louisiana, was an employee of CIT with experience in launching
4 attacks on computer systems and, as set forth below, was involved
5 in the conspiracies to attack Weaknees, Rapid Satellite, and Expert
6 Satellite.

7 UNINDICTED CO-CONSPIRATOR IN CHANDLER, ARIZONA

8 7. An unindicted co-conspirator residing in Chandler,
9 Arizona, was a computer user with experience in launching computer
10 attacks and, as set forth below, was involved in the conspiracy to
11 attack Weaknees and Rapid Satellite.

12 ROBY

13 8. Richard Roby, residing in Celina, Ohio, was a computer
14 user with experience in launching computer attacks and, as set
15 forth below, was involved in the conspiracy to attack Weaknees and
16 Rapid Satellite.

17 WALKER

18 9. Lee Graham Walker, residing in the United Kingdom, was a
19 computer user with experience in launching computer attacks and, as
20 set forth below, was involved in the conspiracy to attack Weaknees
21 and Rapid Satellite.

22 NEXUS TO COMMERCE

23 10. The computers and web-hosting services of Fconet,
24 Weaknees, Rapid Satellite, and Expert Satellite were used in
25 interstate and foreign commerce and communication.

26 //

27 //

28 //

COMPUTER TERMINOLOGY

DDOS Attack

11. A distributed denial of service ("DDOS") attack is a type of malicious computer activity where an attacker causes a network of compromised computers to "flood" a victim computer with large amounts of data or specified computer commands. A DDOS attack typically renders the victim computer unable to handle legitimate network traffic and often the victim computer will be unable to perform its intended function and legitimate users are denied the services of the computer. Depending on the type and intensity of the DDOS attack, the victim computer and its network may become completely disabled and require significant repair.

SynFlood

12. A "SynFlood" is a type of DDOS attack where a computer or network of computers send a large number of "Syn" data packets to a targeted computer. Syn packets are sent by a computer that is requesting a connection with a destination computer. A SynFlood typically involves thousands of compromised computers in a botnet that flood a computer system on the Internet with "Syn" packets containing false source information. The flood of Syn packets cause the victimized computer to use all of its resources to respond to the requests and render it unable to handle legitimate traffic.

HTTPFlood

13. An "HttpFlood" is a type of DDOS attack where a computer or network of computers send a large number of Hyper Text Transfer Protocol ("HTTP") requests to a targeted web server.

//

Bot

14. The term "bot" is derived from the word "robot" and commonly refers to a software program that performs repetitive functions, such as indexing information on the Internet. Bots have been created to perform tasks automatically on IRC servers. Bot also refers to computers that have been infected with a program used to control or launch DDOS attacks against other computers.

Botnet

15. A "botnet" is typically a network of computers infected with bots that are used to control or attack computer systems. Botnets are often created by spreading a computer virus or worm that propagates throughout the Internet, gains unauthorized access to computers on the Internet and infects the system with a particular bot program. The botnet is then controlled by a user, often through the use of a specified IRC channel. A botnet can consist of tens of thousands of infected computers. The unsuspecting infected or compromised computers are often referred to as "zombies" or "drones" and are used in DDOS attacks.

IRC

16. Internet Relay Chat ("IRC") is a network of computers connected through the Internet that allows users to communicate (or chat) with others in real time. IRC users utilize specialized client software to use the service and can access a "channel" which is administered by one or more "operators" or "ops." IRC channels are sometimes dedicated to a topic and are identified by a pound sign and a description of the topic such as "#miamidolphins." IRC channels are also used to control botnets that are used to launch DDOS attacks.

COUNT ONE

[18 U.S.C. § 371]

OBJECT OF THE CONSPIRACY

17. Beginning on an unknown date, and continuing through on or about November 14, 2003, in Los Angeles County, within the Central District of California, and elsewhere, defendant PAUL GARRETT ASHLEY, Jay R. Echouafni, Richard Roby, Lee Graham Walker, and others known and unknown to the United States Attorney, conspired and agreed with each other to knowingly transmit a program, information, code and command, and as a result of such conduct, intentionally cause damage without authorization to a protected computer, and cause loss aggregating more than \$5,000, in violation of 18 U.S.C. § 1030(a)(5)(A)(i).

MEANS BY WHICH THE CONSPIRACY WAS TO BE ACCOMPLISHED

18. The object of the conspiracy was to be accomplished as follows:

a. Echouafni would contact defendant ASHLEY and order him to launch an attack against the web sites Weaknees.Com and RapidSatellite.Com to make them inaccessible on the Internet.

b. Defendant ASHLEY would contact Walker and other co-conspirators and coordinate the DDOS attacks against the particular web site.

c. The co-conspirators would cause a botnet they controlled, or to which they had access, to launch DDOS attacks against the web site, rendering it inaccessible to legitimate users on the Internet.

//

//

1 OVERT ACTS

2 19. In furtherance of the conspiracy, and to accomplish the
3 object of the conspiracy, defendant ASHLEY and others known and
4 unknown to the United States Attorney, committed various overt acts
5 within the Central District of California and elsewhere, including
6 the following:

7 a. On or about October 6, 2003, Echouafni contacted
8 defendant ASHLEY and discussed launching an attack against Weaknees
9 and Rapid Satellite, both competitors of Echouafni's company,
10 Orbit.

11 b. On or about October 6, 2003, defendant ASHLEY
12 contacted Walker and instructed him to launch a DDOS attack against
13 Weaknees.Com and RapidSatellite.Com.

14 c. On or about October 6, 2003, Walker launched a
15 series of SynFlood DDOS attacks against Weaknees.Com and
16 RapidSatellite.Com.

17 d. On or about October 6, 2003, Echouafni paid
18 defendant ASHLEY \$1,000 through the PayPal online payment system.

19 e. On or about October 7, 2003, defendant ASHLEY
20 contacted an unindicted co-conspirator in Chandler, Arizona, and
21 instructed him to launch a DDOS attack against Weaknees.Com and
22 RapidSatellite.Com.

23 f. On or about October 8, 2003, defendant ASHLEY
24 contacted an unindicted co-conspirator in Chandler, Arizona, to
25 discuss the continuing DDOS attacks against Weaknees.Com and
26 RapidSatellite.Com.

27 g. On or about October 8, 2003, an unindicted co-
28 conspirator in Chandler, Arizona, recruited Roby to assist in

1 launching DDOS attacks against Weaknees.Com and RapidSatellite.Com.

2 h. On or about October 9, 2003, defendant ASHLEY
3 contacted an unindicted co-conspirator residing in Metairie,
4 Lousiana, and instructed him to launch a DDOS attack against
5 Weaknees.Com and RapidSatellite.Com.

6 i. On or about October 10, 2003, the co-conspirators
7 launched a series of SynFlood or other DDOS attacks against
8 Weaknees.Com, RapidSatellite.Comm, or the companies hosting these
9 web sites.

10 j. After the DDOS attacks successfully knocked the web
11 sites offline, Echouafni contacted defendant ASHLEY and stated "You
12 guys did a good job."

13 k. On or about October 10, 2003, defendant ASHLEY
14 received another \$1,000 from Echouafni through PayPal.

15 l. On or about October 10, 2003, Echouafni contacted
16 Rapid Satellite's owner and offered to host Rapid Satellite's web
17 site for \$5,000 a month.

18 m. On or about October 11, 2003, defendant ASHLEY
19 transferred \$900 to Walker via PayPal.

20 n. On or about October 14, 2003, the co-conspirators
21 launched HttpFlood DDOS attacks against Weaknees.Com and
22 RapidSatellite.Com.

23 o. In or about December 2003, Echouafni purchased CIT
24 and offered to pay defendant ASHLEY \$120,000 a year to serve as its
25 systems administrator.

26 //

27 //

28 //

COUNT TWO

[18 U.S.C. §§ 1030(a)(5)(A)(i) and 2]

20. Beginning on or about October 6, 2003 and continuing through on or about October 16, 2003, within the Central District of California, within Los Angeles County and elsewhere, defendant PAUL GARRETT ASHLEY aided, abetted, counseled, commanded, induced and procured the knowing transmission of a program, information, code and command, and as a result of such conduct, intentionally caused damage without authorization, to a protected computer, namely, defendant PAUL GARRETT ASHLEY aided and abetted the launching of distributed denial of service attacks against the protected computers of Weaknees.com, and as a result of such conduct, caused loss during a one-year period aggregating at least \$5,000 in value.

COUNT THREE

[18 U.S.C. § 371]

21. The United States Attorney re-alleges and incorporates all of the introductory allegations set forth in paragraphs 1 through 16.

OBJECT OF THE CONSPIRACY

22. Beginning on an unknown date, and continuing through on or about February 16, 2004, in Los Angeles County, within the Central District of California, and elsewhere, PAUL GARRETT ASHLEY and others known and unknown to the United States Attorney, conspired and agreed with each other to knowingly transmit a program, information, code and command, and as a result of such conduct, intentionally cause damage without authorization to a protected computer, and cause loss aggregating more than \$5,000, in violation of 18 U.S.C. § 1030(a)(5)(A)(i).

MEANS BY WHICH THE CONSPIRACY WAS TO BE ACCOMPLISHED

23. The object of the conspiracy was to be accomplished as follows:

a. Echouafni would contact defendant ASHLEY and order him to launch an attack against the web site of Expert Satellite to make it inaccessible on the Internet.

b. Defendant ASHLEY would contact other co-conspirators and coordinate the DDOS attacks against the particular web site.

c. The co-conspirators would cause a botnet they controlled, or to which they had access, to launch DDOS attacks against the web site making it inaccessible to legitimate users on the Internet.

//

OVERT ACTS

24. In furtherance of the conspiracy and to accomplish the object of the conspiracy, defendant PAUL GARRETT ASHLEY and others known and unknown to the United States Attorney, committed various overt acts within the Central District of California and elsewhere, including the following:

25. On or about February 5, 2004, Echouafni directed defendant ASHLEY to launch an attack against the web site for Expert Satellite.

26. Defendant ASHLEY thereafter asked other co-conspirators to launch attacks on the web site for Expert Satellite.

27. From February 6, 2004 through February 12, 2004, Echouafni made repeated requests of an unindicted co-conspirator residing in Metairie, Louisiana to launch DDOS attacks against Expert Satellite to keep Expert Satellite's website inaccessible to customers on the Internet.

28. From February 6, 2004 through February 12, 2004, an unindicted co-conspirator residing in Metairie, Louisiana, launched SynFlood DDOS attacks against Expert Satellite's web site to prevent customers from accessing the site.

29. On or about February 15, 2004, Echouafni contacted an unindicted co-conspirator residing in Metairie, Louisiana, to inform him that he was under investigation by the Federal Bureau of Investigation and advised him to conduct "some housecleaning."

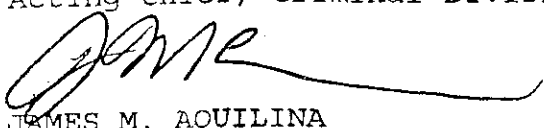
COUNT FOUR

[18 U.S.C. §§ 1030(a)(5)(A)(i) and 2]

30. Beginning on or about February 5, 2004 and continuing through on or about February 16, 2004, within the Central District of California, within Orange County and elsewhere, defendant PAUL GARRETT ASHLEY aided, abetted, counseled, commanded, induced and procured the knowing transmission of a program, information, code and command, and as a result of such conduct, intentionally caused damage without authorization, to a protected computer, namely, defendant ASHLEY aided and abetted the launching of distributed denial of service attacks against the protected computers of Expertsatellite.com, and as a result of such conduct, caused loss during a one-year period aggregating at least \$5,000 in value.

DEBRA W. YANG
United States Attorney

MICHAEL W. EMMICK
Assistant United States Attorney
Acting Chief, Criminal Division


JAMES M. AQUILINA
Assistant United States Attorney
Cyber and Intellectual Property Crimes Section